Hastings Communications and Entertainment Law Journal

Volume 37 | Number 2 Article 6

1-1-2015

Small Steps for Congress, Huge Steps for Online Privacy

Jugpreet Mann

Small Steps for Congress, Huge Steps for Online Privacy

by JUGPREET MANN*

> "We are told that during the Industrial Revolution, there was no such thing as too much coal and iron ore . . . . Today's raw material, the argument goes, is data, and we need as much of it as we can collect."
>
> – Edith Ramirez[1]

---

* Symposium Editor, *Hastings Communications and Entertainment Law Journal*; J.D. Candidate 2015, University of California, Hastings College of the Law; B.S., 2011, Business Administration, University of California, Riverside. I cannot thank my parents, family and friends enough for their love, encouragement, inspiration, and humor. I would also like to thank Comm/Ent editorial staff for their careful work in editing this note.

1. Edith Ramirez, Chairwoman, FTC, Keynote Address at the Technology Policy Institute Aspen Forum: The Privacy Challenges of Big Data: A View From the Lifeguard's Chair 4 (Aug.

I. Introduction

As Internet usage evolved to become embedded into most aspects of daily American life, what would have once been described as paranoia of being constantly watched, may now be a societal norm. In modernity, "[i]nformation about people's moment-to-moment thoughts and actions, as revealed by their online activity, can change hands quickly."[2] The U.S. Census Bureau ("Bureau") reported that, "[i]n 2011, more Americans connected to the Internet than ever before," with 71.7 percent of American households that responded to the census having accessed the Internet.[3] The Bureau found that this increased Internet usage was facilitated by the evolution of technology, as it provided many new ways for individuals to utilize their computers and access the Internet.[4] Correspondingly, on a global scale, the International Data Corporation ("IDC") found that the information available in the digital universe would be 1.8 trillion gigabytes in 2011 and "more than doubl[e] every two years."[5]

To monetize this vast resource, companies have developed innovative ways to both collect and create value from information they receive.[6] Essentially, the ability to create value from data has directly incentivized companies to consistently eviscerate online privacy.[7] The term "Big Data" can be broadly defined as the "capture, management, and analysis of data that goes beyond typical structured data, which can be queried by relational database management systems."[8] Although the process of collecting and utilizing such data has resulted in significant benefits, many recent cases have exemplified that companies are overreaching and thereby intruding into the privacy of individuals.[9]

The most disturbing aspect of data creation is that the information created about individuals significantly outweighs the amount of

19, 2013), *available at* https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-challenges-big-data-view-lifeguard%E2%80%99s-chair/130819bigdataaspen.pdf.

2. Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J., July 30, 2010, *available at* http://www.wsj.com/articles/SB10001424052748703940904575395073512989404.

3. THOM FILE, U.S. CENSUS BUREAU, COMPUTER AND INTERNET USE IN THE UNITED STATES, POPULATION CHARACTERISTICS 1 (2013), *available at* http://www.census.gov/prod/2013pubs/p20-569.pdf.

4. *Id.* at 6.

5. JOHN GANTZ & DAVID REINSEL, EMC CORP., EXTRACTING VALUE FROM CHAOS 1 (2011), *available at* http://www.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf.

6. *Id.* at 2.

7. Angwin, *supra* note 2.

8. Sam B. Siewert, *Big Data in the Cloud*, IBM, at 2 (July 9, 2013), *available at* http://www.ibm.com/developerworks/library/bd-bigdatacloud/.

9. *See, e.g.*, FTC v. Toysmart.com, LLC, No. 00-CV-11341, 2000 U.S. Dist. LEXIS 21963 (D. Mass. Aug. 21, 2000); *In re* Google Inc., Docket No. C-4336 (F.T.C. Oct. 13, 2011).

information individuals create themselves.[10] Since this information is not of a physical nature, an average individual has no way of confirming such information directly. Although each state provides a right of action for invasion of privacy, Big Data poses significant legal challenges because the right to privacy is impaired in the online context.[11] Therefore, even if an individual realizes that his or her information is being tracked and recorded, the individual has limited courses of action.

An entire industry of data brokerage firms has emerged with the purpose of collecting information to resell it.[12] Processes, such as Online Behavioral Advertising in which companies use acquired information to provide individuals with specifically identifiable ads or content, have proven to be quite profitable.[13] When companies identify an individual by a random identification number and use that individual's online activity to make educated guesses about their interests and characteristics, a privacy issue does not seem to arise. Privacy issues do arise, however, when personal information is gathered or de-identified.[14] This problem is best exemplified by a recent World Privacy Forum investigation that revealed that data brokers sold to marketers lists of rape victims, seniors with dementia, individuals suffering from HIV or AIDS, addresses of police officers, and individuals with drug and alcohol addictions.[15]

An individual has significantly less online privacy than he would reasonably expect. To alleviate unscrupulous invasions of privacy, Congress should take an empirical approach to provide significant protection for the information entered online that an individual has taken measures to keep private or has a reasonable expectation will be kept private. According to IDC findings, less than one-third of information is minimally protected and "only about half the information that should be protected is protected."[16]

10. GANTZ & REINSEL, *supra* note 5, at 1.

11. *See The Privacy Torts: How U.S. State Law Quietly Leads the Way in Privacy Protection*, PRIVACILLA, app. (July 2002), http://www.privacilla.org/releases/Torts_Report.html (listing key cases and statutes for privacy torts recognized in each of the fifty states).

12. Press Release, FTC, FTC to Study Data Broker Industry's Collection and Use of Consumer Data (Dec. 18, 2012), https://www.ftc.gov/news-events/press-releases/2012/12/ftc-study-data-broker-industrys-collection-use-consumer-data.

13. *Understanding Online Behavioral Advertising (OBA)*, TRUSTE, http://www.truste.com/consumer-privacy/about-oba/ (last visited Dec. 27, 2013).

14. *Re-identification*, ELEC. PRIVACY INFO. CTR., https://epic.org/privacy/reidentification/#intro (last visited Mar. 18, 2015) [hereinafter ELEC. PRIVACY INFO. CTR, *Re-identification*].

15. Melanie Hicken, *Data Brokers Sell Lists of Rape Victims, AIDS Patients, Privacy Group Finds*, CNN (Dec. 18, 2013), http://money.cnn.com/2013/12/18/pf/data-broker-lists/.

16. GANTZ & REINSEL, *supra* note 5, at 1.

The federal government's current approach to online privacy has created significant gaps in laws protecting online privacy.[17] The government has also been struggling to keep pace with the rapidly expanding uses of personal data generated from innovative technology geared towards delivering a personal experience to each consumer.[18] Further, the use of section 5 of the Federal Trade Commission Act (the "FTCA") to address online privacy issues is an ineffective way to enforce the statute. First, the statutory language is inherently vague and second, the Federal Trade Commission (the "FTC") has been consistently struggling to expand its authority through precedent.[19]

This note will argue that Congress should move past its hesitancy from enacting baseline legislation and take preliminary steps to better strike a balance between consumers' constitutional right to privacy and international economic growth. Congress can strike this balance by enacting key legislation that mandates transparent information gathering practices of companies, incentivizes companies to adhere to stronger privacy legislations, strengthens enforcement powers of the FTC, and establishes a committee to focus on further commercial data privacy efforts.

Part II of this note will provide background of Big Data and address how companies collect and create value from personal information. It will also trace the history of privacy, address Congress' current approach to online privacy, and address how the states and other nations have approached online privacy. Next, Part III of this note will analyze the need to improve current U.S. legislation, assess the benefits and consequences of the various approaches, and propose small steps that Congress can take but that will make a significant step towards online privacy while broader legislation is debated. Finally, Part IV will conclude by urging Congress to take small steps now, which will constitute significant progression towards the protection of online privacy.

---

17. DEP'T OF COMMERCE INTERNET POLICY TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK 12 (2010), *available at* http://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162 010.pdf.

18. *See id.* at 1 (explaining the "lag between developments in intensive uses of personal information and the responses of current systems of privacy regulation around the world"); *see* Ioana Rusu, *Consumer Union Filing With Federal Trade Commission on Online Privacy*, CONSUMERS UNION, http://consumersunion.org/research/consumers-union-filing-with-federal-trade-commission-on-online-privacy/ (last visited Mar. 5, 2014).

19. *See generally* JOSHUA D. WRIGHT, FTC, THE NEED FOR LIMITS ON AGENCY DISCRETION & THE CASE FOR SECTION 5 GUIDELINES (Dec. 16, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/need-limits-agency-discretion-case-section-5-guidelines/131216section5_ wright.pdf; *see also* Karin A. DeMasi & Jonathan J. Clarke, Cravath, Swaine & Moore, LLP, *Section 5 of the FTC Act and the End of Antitrust Modesty,* BLOOMBERG L. REP., at 3–6 (June 25, 2010), http://www.cravath. com/files/Uploads/Documents/Publications/3233999_1.pdf.

II. Background

Big Data is invisible, intangible, and exponentially multiplying, with the ability to depict a person's thoughts, share the person's location, and inform others about the individual's personal life. Furthermore, Big Data has become significantly cheaper to collect. The potential value of Big Data to benefit companies is vast, whereas the costs for extracting such data are low. Companies can generally employ collected information to boost performance, make better management decisions, further customize products or services to individual needs, improve decision making, improve development of upcoming products and services, predict customer habits and election trends, further understand the risk inherent in undertaking insurance, and predict customer profitability.[20] The costs associated with data collection are minimal because hard disk space and bandwidth are inexpensive.[21] Recent statistics found that an average Fortune 100 company could increase its revenue by two billion dollars from a ten-percent increase in usability of data.[22] It was further estimated that the healthcare industry could save $300 billion through efficient implementation of Big Data.[23] Companies spent $3.2 billion on Big Data in 2010, and it was predicted that this number would rise to $16.9 billion by 2015.[24]

Another way to create value from Big Data is behavioral advertising, which is the "collection of information about online activities and Web viewing behaviors, over time and across non-affiliate websites," to match advertisements with consumer interests.[25] With the advancement of marketing, it is important to realize that the visual inconvenience of "annoying advertisements" is no longer the only fee for keeping websites free.[26] Traditional online advertising consisted of individual purchasing

20. James Manyika et al., *Big Data: The Next Frontier for Innovation, Competition, and Productivity*, MCKINSEY & CO. (May 2011), http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation.

21. John Pethica, *The True Cost of Data Collection*, COMPUTING (June 25, 2009), http://www.computing.co.uk/ctg/opinion/1829953/the-true-cost-collection.

22. Marc Compeau, *Data for Dummies, What Does Your Small Business Need? (Part 1)*, FORBES (July 30, 2013), http://www.forbes.com/sites/marccompeau/2013/07/30/data-for-dummies-what-does-your-small-business-need-part-1/.

23. *Id.*

24. *Id.*

25. *DMA Online Behavioral Advertising (OBA) Compliance Alert & Guidelines for Interest-Based Advertising*, DMA, http://www.dmaresponsibility.org/privacy/oba.shtml (last visited Jan. 13, 2014).

26. Pratap Chatterjee, *How Private Tech Companies Are Collecting Data on You and Selling Them to the Feds for Huge Profits*, ALTERNET (Dec. 28, 2013), http://www.alternet.org/civil-liberties/how-private-tech-companies-are-collecting-data-you-and-selling-them-feds-huge.

advertisements on webpages that were similar to the product or service they were offering.[27] Now, advertisers are paying tracking companies, data brokers, and advertising networks[28] to determine more effective and relevant advertising locations based upon consumer interest and preferences.[29]

Privacy is a significant concern for Big Data because companies use improper mechanisms to collect data, store collected data, and utilize such data.[30] Companies routinely install tracking technology not only in computers, but also in various data devices.[31] Many tools for data collection exist, but common techniques include Page Tags, Logfiles, and Cookies.[32] Page Tags refer to the placement of a "beacon" code on a website to acquire data from a visitor's web browser.[33] Logfiles are records of requests that a visitor makes onto a web server.[34] Cookies are text files that are placed onto a computer from visited websites for purposes of later anonymously identifying a user, and they essentially transfer information in the background.[35]

Despite such a vigilant nature, tracking technology is not inherently malicious.[36] Problems arise when tracking mechanisms are unknown to the user,[37] marketed to the websites within free software, not widely known, and have the power to track a person anywhere.[38] Cookies best exemplify these concepts because they make website usage convenient for an individual,[39] and allow for creation of revenue through targeted online advertising.[40] Cookies can violate an individual's reasonable expectation of privacy when they collect information without the user's knowledge, when they are used differently than what the developer states in its privacy policy, or when a third-party cookie is sent from a different website than

27. Angwin, *supra* note 2.

28. *Id.*

29. DMA, *supra* note 25.

30. Chatterjee, *supra* note 26.

31. *Id.*

32. BRIAN CLIFTON, OMEGA DIGITAL MEDIA, WEB TRAFFIC DATA SOURCES & VENDOR COMPARISON 2 (May 20, 2008), *available at* http://www.ga-experts.com/web-data-sources.pdf.

33. *Id.* at 3.

34. *Id.*

35. *Id.* at 5; Wayne Porter, *Internet Cookies—Spyware or Neutral Technology*, SPYWARE GUIDE, http://www.spywareguide.com/articles/internet_cookies_spyware_or_ne_57.html (last visited Dec. 27, 2013).

36. CLIFTON, *supra* note 32, at 3–4.

37. *Id.*

38. Angwin, *supra* note 2.

39. CLIFTON, *supra* note 32, at 4.

40. DMA, *supra* note 25.

the one visited.[41] Further, a flash cookie is a type of cookie that can circumvent the user's attempt to delete it by reinstalling itself.[42]

Companies are not well equipped to store collected information and, as many cases demonstrate, the lack of secure data repository has left their databases vulnerable.[43] In April 2011, Sony's Playstation Network and Qriocity streaming service user account information was compromised when hackers gained access to users' names, home addresses, email addresses, birthdates, and login information.[44] Sony Pictures was also attacked later that same year, which resulted in the leak of over 1 million user accounts, 75,000 music codes, and 3.5 million coupons.[45] LexisNexis, Dunn & Bradstreet, and Kroll Background America are all data brokerages that were hacked in 2013.[46] Target was hacked in late 2013 when customer names, credit and debit card numbers, expiration dates, and security codes were taken.[47]

In addition to external threats to privacy, companies themselves can also violate individuals' privacy rights by gathering information without their awareness, using acquired information for a purpose other than the one for which the information was originally provided, and selling the information acquired for personal purposes without permission.

A 2010 *Wall Street Journal* ("WSJ") investigation of the fifty most popular U.S. websites found a total of 3180 tracking files on its test computer. Companies in the business of tracking web users installed more than two-thirds of these tracking files to sell collected information.[48] The WSJ investigation further found that some companies, such as Microsoft and Comcast, were unaware of how such files got onto their websites.[49]

Facebook is a prime example of a company that used acquired information for purposes other than the purpose for which such information

41. Angwin, *supra* note 2.

42. *Id.*

43. Chatterjee, *supra* note 26.

44. Patrick Seybold, *Update on Playstation Network and Qriocity*, PLAYSTATION BLOG (Apr. 26, 2011), http://blog.us.playstation.com/2011/04/26/update-on-playstation-network-and-qriocity/.

45. Christina Warren, *Sony Pictures Website Hacked,* CNN (June 3, 2011), http://www.cnn.com/2011/TECH/web/06/03/sony.pictures.hacked.mashable//.

46. Byron Acohido, *Lexis Nexis, Dunn & Bradstreet, Kroll Hacked*, USA TODAY, Sept. 26, 2013, *available at* http://www.usatoday.com/story/cybertruth/2013/09/26/lexisnexis-dunn—bradstreet-altegri tyalte grity-hacked/2878769/.

47. George Wallace, *Target Credit Card Hack: What You Need to Know*, CNN MONEY (Dec. 23, 2013), http://money.cnn.com/2013/12/22/news/companies/target-credit-card-hack/.

48. Angwin, *supra* note 2.

49. *Id.*

was originally provided to them.[50] The Electronic Privacy Information Center ("EPIC") and five other interest groups filed a complaint with the FTC against Facebook, alleging that proposed changes to the Facebook policy would allow the company to utilize user information automatically for commercial purposes, unless users denied the company permission.[51] This proposed change was the result of a $20-million settlement from a 2011 lawsuit, which alleged that Facebook used its users' "personal information for commercial purposes without consent or compensation."[52]

In 2013, a former test-taker filed a class action lawsuit against ACT, Inc. and the College Board—companies that administer national tests for high school students—for selling students' personal data without permission.[53] The complaint alleged that although the companies asked permission to share personal data, they did not disclose that such information would be sold to purchasers for thirty-three cents per student.[54]

A. Foundation of Privacy in the United States

The United States Constitution does not explicitly mention the right to privacy.[55] It was first addressed in legal scholarship, as opposed to constitutional jurisprudence.[56] In 1890, Samuel Warren and Louis Brandeis published the influential law review article, *The Right to Privacy*, in which they articulated the "right to be let alone."[57] The article called for the expansion of an individual's common law protection in person and property to meet emerging demands of society caused by "political, social, and economic changes" of the time.[58]

Thereafter, Judge Brandeis' 1928 dissenting opinion in *Olmstead v. United States* asserted that the Framers of the Constitution intended that the "right to be let alone" protect "Americans in their beliefs, their thoughts,

50. Jessica Guynn, *Facebook Under Fire From Privacy Watchdogs over 'Sponsored Stories' Ads*, L.A. TIMES, 1, Sept. 4, 2013, *available at* http://articles.latimes.com/2013/sep/04/business/la-fi-tn-facebook-under-fire-from-privacy-watchdogs-over-sponsored-stories-ads-20130904.

51. *Id.*

52. *Id.*

53. Andrew Harris, *SAT and ACT College Test Companies Sued Over Data Sales*, BLOOMBERG BUS. (Oct. 31, 2013), http://www.bloomberg.com/news/articles/2013-10-31/sat-and-act-college-test-companies-sued-over-data-sales.

54. *Id.*

55. Farron Brougher, *The Short History of the Right to Privacy*, EXAMINER (Jan. 4, 2012), http://www.examiner.com/article/the-short-history-of-the-right-to-privacy.

56. *Id.*

57. *Id.*; Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

58. *Id.* at 193.

their emotions and their sensations."[59] He described this right as being "the most comprehensive of rights and the right most valued by civilized men," for the protection of which "every unjustifiable intrusion by the Government upon the privacy of the individual . . . must be deemed a violation of the Fourth Amendment."[60] Finally, in the 1965 *Griswold v. Connecticut* decision, the United States Supreme Court recognized a constitutional right to privacy when it held that "[s]pecific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees," which "create zones of privacy."[61]

B. Congress's Approach to Online Privacy

The United States has currently taken a sectorial approach to online privacy, which facilitates "tailoring of legislative rules to fit specific industries, but it does not apply broadly to all types of data across all sectors" like a baseline approach would.[62] The following is a list of some industry-specific laws that Congress has enacted:

The Electronic Communications Privacy Act of 1986 serves the purpose of creating "a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement."[63]

The Children's Online Privacy Protection Act requires that commercial website operators and online services provide notice and obtain parental consent prior to collecting personal information from children under thirteen years of age.[64]

The Gramm-Leach-Bliley Act requires financial service companies to securely store personal financial information, to advise customers of the policies on sharing such information, and to provide customers an opportunity to opt out of sharing some personal information with other companies.[65]

The Health Insurance Portability and Accountability Act establishes a national standard for covered entities that balances the need to protect health information while facilitating the flow of such information to be able to provide quality health care.[66] This Act addresses the technical and non-

59. Olmstead v. United States, 277 U.S. 438, 454 (1928).

60. *Id.*

61. Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

62. DEP'T OF COMMERCE INTERNET POLICY TASK FORCE, *supra* note 17, at 12.

63. *Electronic Communications Privacy Act*, ELEC. PRIVACY INFO. CTR., http://epic.org/privacy/ecpa/ (last visited Dec. 29, 2013).

64. *Privacy Laws*, CAL. DEP'T OF JUSTICE, OFFICE OF THE ATT'Y GEN. http://oag.ca.gov/privacy/privacy-laws (last visited Jan. 2, 2014).

65. *Id.*; *The Gramm-Leach-Bliley Act*, ELEC. PRIVACY INFO. CTR., http://epic.org/privacy/glba/ (last visited Dec. 29, 2013).

66. *Summary of the HIPAA Privacy Rule*, U.S. DEP'T. OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/ (last visited Mar. 21, 2015).

technical safeguards that must be employed to protect certain health information that is held or transferred in electronic form,[67] and protects identifiable information being used to assess patient safety.[68]

The Privacy Act of 1974 is binding upon federal agencies and records in their possession, and prohibits the disclosure of records that could be retrieved by personal identifiers without written consent from the individual whose information would be in the record, unless one of twelve listed exceptions applied.[69]

The Computer Fraud and Abuse Act of 1986 was enacted to ensure that "federal computers, banks, and computers used in interstate and foreign commerce" would be protected "from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud" by employing criminal and civil penalties.[70]

The Credit Reporting Act protects consumer rights by requiring consumer credit reporting agencies to disclose to individuals their own credit file upon request, prohibiting the agencies from sharing such information to any party unless they have a permissible purpose, and mandating prompt investigation upon notification by an individual that his or her file contains inaccurate information.[71]

As the foregoing legislations demonstrate, Congress has essentially chosen a circumstance-specific approach in which it enacts legislation in response to certain events. This approach has resulted in strong industry-specific laws but minimal protection for information that falls outside those categories.[72]

C. Federal Trade Commission

The Federal Trade Commission Act ("FTCA") established the Federal Trade Commission ("FTC") in 1914 with the original purpose of preventing unfair competition methods.[73] Congress has since enacted the 1938 prohibition against "unfair and deceptive acts or practices," directing the FTC to administer specific consumer protection laws, and has empowered the FTC to adopt industry-wide regulatory rules.[74]

67. *Id.*

68. *The Privacy Act*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/foia/privacy/ (last visited Mar. 5, 2014).

69. *Id.*

70. CHARLES DOYLE, COMPUTER FRAUD AND ABUSE LAWS: AN OVERVIEW OF FEDERAL CRIMINAL LAWS, at vii (2002).

71. EQUIFAX, *FRCA Summary of Rights*, https://help.equifax.com/app/answers/detail/a_id/36 (last visited Dec. 30, 2013).

72. DEP'T OF COMMERCE INTERNET POLICY TASK FORCE, *supra* note 17, at 12.

73. *About the FTC*, FTC, http://www.ftc.gov/about-ftc (last visited Dec 30, 2013).

74. *Id.*

Specifically, section 5 of the FTCA provides the FTC with authority to "prevent persons, partnerships, or corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[75] This statute has subsequently been interpreted as prohibiting certain privacy invasions.[76]

The FTCA specifies that "unfair or deceptive acts or practices" include acts involving foreign commerce that are "likely to cause reasonably foreseeable injury within the United States or involve material conduct occurring within the United States."[77] The FTCA further provides that the FTC can declare an act to be unfair if the "act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[78] This "unfairness" prong has been criticized as insufficient to provide companies with guidance on what is acceptable conduct with respect to consumer privacy and, therefore, resulting in application on a case-by-case basis.[79] On the contrary, application of the "deceptive" prong has provided clarity by notifying companies that they must not make untrue or misleading privacy statements.[80] The FTC has stated that it "will find an act or practice deceptive if there is a misrepresentation, omission, or other practice that misleads the consumer acting reasonably in the circumstances to the consumer's detriment."[81]

D. FTC's Current Standing

The FTC has consistently supported self-regulation.[82] In fact, in its 1998 testimony before Congress, the FTC recommended that Congress should not pass legislation at that time.[83] Further, in 2000, even when the FTC recommended that Congress pass legislation, it still emphasized that

75. 15 U.S.C. § 45(a)(2) (2011).

76. *About FTC, supra* note 73; Ramirez, *supra* note 1, at 3.

77. 15 U.S.C. § 45(a)(4)(A)(i).

78. *Id.* § 45(n).

79. Alan L. Friel, *Why We Don't Need the FTC on Big Data Lifeguard Duty*, ADVERTISING AGE (Oct. 8, 2013), http://adage.com/article/privacy-and-regulation/ftc-big-data-lifeguard-duty/244128/.

80. *Id.*

81. FTC, POLICY STATEMENT ON DECEPTION (1983), *available at* https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.

82. FTC, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, A REPORT TO CONGRESS 3 (2000) [hereinafter FTC REPORT ON FAIR INFORMATION PRACTICES], *available at* https://www.ftc.gov/sites/ default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf.

83. *Id.* at 3.

industry self-regulation, coupled with consumer and business education, should be central in such legislation.[84] As a practical result of promoting self-regulation, however, the FTC lacks the authority to mandate information practice policies.[85] The FTC has consistently called for industry efforts to implement fair information practice principles.[86] The U.S. Secretary Advisory Committee on Automated Personal Data Systems issued its 1973 report *Records, Computers, and the Rights of Citizens,* which initially introduced Fair Information Practices as "principles for protecting the privacy of personal data in record-keeping systems."[87] Numerous international organizations have since endorsed versions of the Fair Information Practice Principles ("FIPPS").[88] The FTC first supported the principles of Notice, Choice, Access, and Security in its 1998 report entitled *Privacy Online: A Report to Congress.*[89]

"Notice" requires websites to inform consumers with "clear and conspicuous notice of their information practices."[90] "Choice" requires websites to offer consumers choices as to how companies utilize personal information, in contexts other than one authorized by the consumer.[91] "Access" requires websites to offer consumers reasonable access, opportunity to review, and opportunity to correct or delete information the website collected about them.[92] "Security" requires websites to take reasonable measures to safeguard collected information.[93]

One specific manner in which corporations can comply with the FTC is via the online privacy seal programs. These programs allow their licensees to display a privacy seal on their websites in exchange for implementation of certain fair information practice principles and submission to monitoring.[94]

In 2010, the FTC noted in its preliminary report that the "emphasis on notice and choice alone ha[d] not sufficiently accounted for other widely recognized fair information practices such as access, collection limitation,

84. *Id.* at 36.

85. *Id.* at 34.

86. *Id.* at 3, 5, 34.

87. ROBERT GELLMAN, FAIR INFORMATION PRACTICES: A BASIC HISTORY 2 (Feb. 11, 2015), *available at* http://bobgellman.com/rg-docs/rg-FIPShistory.pdf.

88. *Id.* at 7.

89. FTC, PRIVACY ONLINE: A REPORT TO CONGRESS, 7–10 (1998), *available at* https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

90. FTC REPORT ON FAIR INFORMATION PRACTICES, *supra* note 82, at iii.

91. *Id.*

92. *Id.*

93. *Id.*

94. *Id.* at 6.

purpose specification, and assuring data quality and integrity."[95] In 2012, the FTC released a final version of its 2010 preliminary report that provides its final best practices for businesses to "protect the privacy of American Consumers and give them greater control over the collection and use of their personal data."[96] This final report included a call to action for Congress to consider enacting baseline privacy legislation, repeated its call for data security legislation, and impelled the industry to accelerate the pace of self-regulation.[97] The FTC retained its recommendation that companies handling consumer data implement "Privacy by Design," "Simplified Choice for Businesses and Consumers," and "Greater Transparency."[98] Privacy by Design refers to the principle that companies should promote organization-wide consumer privacy at each stage of development of products and services.[99] Simplified Choice for Businesses and Consumers provides that when a company is required to afford a consumer the option to decide how their data is used, the company should provide such choice at a "relevant time and in a prominent manner."[100] Greater Transparency calls for more comprehensible privacy practices and reasonable access to consumer data, and encourages that all stakeholders should expand efforts to educate consumers about commercial data privacy practices.[101]

The FTC, however, made key changes to their recommendations between the 2010 preliminary report and the 2012 final report.[102] The FTC narrrowed its recommendation as to which companies should implement their framework. The 2010 report recommended implementation of the framework by "all commercial entities that collect or use consumer data that can be linked to specific consumer, computer, or other device."[103] The 2012 report acknowledged the burden that the framework may impose on small businesses and consequently exempted from its framework "companies that collect only non-sensitive data from fewer than 5,000

95. FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 20 (2012) [hereinafter FTC REPORT ON PROTECTING CONSUMER PRIVACY], *available at* https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

96. Press Release, FTC, FTC Issues Final Commission Report on Protecting Consumer Privacy (Mar. 26, 2012), http://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy.

97. FTC REPORT ON PROTECTING CONSUMER PRIVACY, *supra* note 95, at i–ii.

98. *Id.* at i.

99. *Id.*

100. *Id.* at i, 27.

101. *Id.*

102. *Id.* at ii.

103. *Id.* at iv.

consumers a year, provided they do not share the data with third parties."[104] The 2012 report also made clear that data is not "reasonably linked" so long as a company "(1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits to not try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data."[105] The report also abolished the five categories of "commonly accepted" information collection and use practices that the 2010 preliminary report had listed as instances in which a company would not be required to present consumers with a choice about how their data is utilized.[106] The FTC then adopted the "context of the interaction" standard, which provides that companies need not provide choice prior to collecting and utilizing consumer data for practices "consistent with the context of the transaction, consistent with the company's relationship with the consumer, or as required or specifically authorized by law."[107] The FTC emphasized the need for legislation applicable to data brokers that would provide transparency, control, and reasonable access to data.[108] The report also highlighted that the FTC would focus throughout the following year on "Do Not Track," improved privacy protections for mobile services, practices of data brokers, practices of large platform providers, and development of sector-specific codes of conduct.[109]

E. State Laws Regulating Online Privacy

In addition to federal legislation, many states provide statutory protection to online privacy. California, for example, has been a leader in online privacy laws.[110] On July 19, 2012, the California Department of Justice created the Privacy Enforcement and Protection Unit to enforce state and federal privacy laws and to act as a resource for consumers.[111] California has also enacted several statutes, including the California Online Privacy Protection Act of 2003, the California Consumer Protection

104. *Id.*

105. *Id.*

106. *Id.*

107. *Id.*

108. *Id.* at v.

109. *Id.* at v-vi (stating that "Do Not Track" is a system composed of "tools that consumers can use to signal that they do not want to be tracked").

110. Somini Sengupta, *No U.S. Action, So States Move on Privacy Law*, N.Y. TIMES, Oct. 30, 2013, at A1.

111. Sidley Austin LLP, *California Attorney General Creates Privacy Enforcement and Protection Unit; National Attorneys General Internet Privacy Initiative* (July 26, 2012) http://www.sidley.com/news/california-attorney-general-creates-privacy-enforcement-and-protection-unit-national-attorney-general-internet-privacy-initiative-07-25-2012.

Against Consumer Spyware Act, and the Data Breach Notification Law.[112] The California Online Privacy Protection Act of 2003 requires operators of commercial websites or online services that collect personally identifiable information about California residents to utilize the operators' websites to conspicuously post a privacy policy.[113] This privacy policy must, among other things, identify categories of personally identifiable information collected and categories of third parties with whom such information may be shared.[114] The California Consumer Protection Against Consumer Spyware Act provides that an unauthorized person may not willfully cause software to be copied onto a consumer's computer that, among other things, collects personally identifiable information through intentionally deceptive means.[115]

Further, California's Data Security Breach Reporting Law requires businesses to notify any California resident whose personal information is reasonably believed to have been compromised by an unauthorized person.[116] If any business must issue such notification to over 500 California residents arising from a single breach, it must submit a sample copy of the security breach notification to the Attorney General.[117] Nevada and Minnesota also both prohibit Internet service providers ("ISPs") from disclosing certain information concerning their customers without consent.[118] Minnesota provides a list of "personally identifiable information" that must not be disclosed.[119] Nevada takes a further step by explicitly mandating ISPs to keep confidential "all information concerning a subscriber, other than electronic mail addresses."[120]

F. How Other Nations Address Online Privacy

Other nations have distinct approaches to online privacy. For example, the Personal Information Protection and Electronic Documents Act ("PIPEDA"), effective as of 2004, is Canada's law regulating online

112. CAL. DEP'T OF JUSTICE, *supra* note 64.

113. Scott P. Cooper et al., *State Privacy Laws*, *in* PROSKAUER ON PRIVACY: A GUIDE TO PRIVACY AND DATA SECURITY LAW IN THE INFORMATION AGE § 5:2.1(A) (Practicing Law Inst. 2014), *available at* http://www.pli.edu/public/booksamples/11513_sample5.pdf.

114. *Id.*

115. CAL. BUS. & PROF. CODE §§ 22947–22947.6 (West 2015).

116. *Data Security Breach Reporting*, CAL. DEP'T. OF JUSTICE, OFFICE OF ATT'Y GEN., https://oag.ca.gov/ecrime/databreach/reporting (last visited Mar. 22, 2015); *see also* CAL. CIV. CODE §§ 1798.29(a), 1798.82(a) (West 2015).

117. *Data Security Breach Reporting*, *supra* note 116; *see also* CAL. CIV. CODE §§ 1798.29(e), 1798.82(f).

118. Cooper, et al., *supra* note 113, § 5:2.1(B).

119. *Id.*; *see also* MINN. STAT. § 325M.01(5) (2014).

120. *Id.*; *see also* NEV. REV. STAT. § 205.498 (2011).

privacy.[121] PIPEDA applies to commercial organizations that collect, use, or disclose personal information.[122] The Act requires that such practices be carried out via fair and lawful means, with consent, and solely for purposes stated in a reasonable manner.[123] This requirement provides a right of access to the consumer to ensure that information held about the person is accurate, updated, and deleted when no longer necessary for its original purpose.[124] Under this framework, organizations are required to delegate responsibility of resolving privacy issues to a specific staff member.[125] Although an affected individual is encouraged to express his or her complaint with the staff member first, the individual retains the option to file a complaint with the Primary Commissioner of Canada for non-compliance.[126] Then, for dissatisfaction with the Privacy Commissioner, the individual may proceed to take his or her complaint to Federal Court of Canada.[127]

The European Union ("EU") currently operates under the European Union Data Protection Directive ("Directive"), effective October 1998, which provides a regulatory framework for movement of personal data across EU member countries and provides a baseline of security.[128] The Directive is applicable to personal data that is processed by automatic means, which is part of, or intended to form part of, a filing system.[129] The Directive requires each EU member state to enact its own local "data protection" law that adopts the Directive and "prohibits sending personal data to any country without the 'level of [data] protection' considered 'adequate.'"[130] Personal data is broadly defined to be any information related to an identifiable natural person, which is a person that can be directly or indirectly identified by reference to specific factors.[131] Process of personal data is broadly defined to include "any operation or set of

121. OFFICE OF PRIVACY COMM'R OF CAN., THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT, *available at* http://www.priv.gc.ca/information/02_05_d_08_e.asp (last visited Jan. 2, 2014).

122. *Id.*

123. *Id.*

124. *Id.*

125. *Id.*

126. *Id.*

127. *Id.*

128. Christopher Wolf & Timothy Tobin, *Privacy Laws*, *in* PROSKAUER ON INTERNATIONAL LITIGATION AND ARBITRATION § III.A, *available at* http://www.proskauerguide.com/law_topics/28/III/:pf (last visited Jan. 2, 2014).

129. *EU Data Protection Directive (Directive 95/46/EC)*, TECHTARGET, http://searchsecurity.techtarget.co.uk/definition/EU-Data-Protection-Directive (last visited Jan. 2, 2014).

130. Wolf & Tobin, *supra* note 128, § III.A.2.

131. *Id.* § III.A.3.a–.b.

operations which is performed upon personal data, whether or not by automatic means."[132]

The Directive specifies "principles relating to data quality" with which entities must comply when processing personal data.[133] These data principles include processing of data "fairly and lawfully" for a specific purpose.[134] Entities must not collect the data excessively in relation to such purpose.[135] The data must be accurate and kept "no longer than necessary," and a controller must implement measures that ensure the data is processed with adequate security.[136] Further, "'decision[s]' from data processing cannot be 'based solely on automated processing of data' that 'evaluate[s] personal aspects.'"[137] In addition, the processing must also be either "consented-to or 'necessary.'"[138] The Directive further mandates informing individuals about their on-file data, providing access, correcting any errors, outlawing secretive processing of personal data, and that each member state create a Data Protection Authority to administer the data protection law.[139]

On January 25, 2012, however, the EU proposed a draft of the European General Data Regulation to replace the Data Protection Directive.[140] The proposed regulation, if passed into law, will be directly applicable to all member states so as to replace the existing twenty-seven different national regulations with a single umbrella law.[141] This law will further encompass activities of data processors and extend to all foreign companies processing data of EU citizens.[142] The regulation will require that data controllers have transparent and easily accessible policies conspicuously highlighting their data processing activities and rights of

132. *Id.* § III.A.3.c.

133. Council Directive 95/46/EC, art. 6, 1995 O.J., (L 281), *available at* http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31995L0046; Wolf & Tobin, *supra* note 128, § III.B (listing seven data quality principles: fairness, specific purpose, restricted, accurate, destroyed when obsolete, security, automated processing).

134. Council Directive 95/46/EC, art 6, § 1(a)–(b).

135. *Id.* § 1(c).

136. *Id.* §§ 1(d)–(e), 2.

137. Wolf & Tobin, *supra* note 128, § III.B.7.

138. *Id.* § III.C.2.

139. *Id.* § III.F.

140. *New Draft European Data Protection Regime*, M LAW GRP. (Feb. 2, 2012), http://www.mlawgroup.de/news/publications/detail.php?we_objectID=227. The Council of the European Union expects to conclude the legislative negotiations "by the end of 2015, a much-touted target date." John Bowman, *Regulation: A Tipping Point Has Been Reached*, THE INT'L ASS'N OF PRIVACY PROF'LS (Nov. 7, 2014), https://privacyassociation.org/news/a/eu-data-protection-regulation-a-tipping-point-has-been-reached/.

141. M. LAW. GRP., *supra* note 140.

142. Luke Dixon, Greenberg Traurig LLP, *The Draft EU Data Protection Regulation: Where Are We Now, and Where Are We Going?*, LEXOLOGY (Sept. 11, 2013), http://www.lexology.com/library/detail.aspx?g= 7cef61cf-0988-4f0f-9c2b-3d3e8ab6f266.

data subjects.[143] Such a requirement will provide for an opt-in approach to obtaining consent, "right of portability" to facilitate transfer of data amongst online service providers upon request, and "right to be forgotten" so that an individual has the opportunity to erase all data pertaining to them.[144] "Public sector bodies," private sector businesses employing over 250 people, and "businesses whose core activities consist of processing operations which require regular and systematic monitoring of data subjects" will be required to appoint a data protection officer to oversee compliance.[145] Companies will have to provide notice to any individual whose information is compromised, and to EU data protection authorities, within twenty-four hours per breach of acquired information.[146] The Data Protection Authorities will retain the right to impose a penalty upon breach of up to two percent of the company's worldwide turnover.[147]

On May 26, 2012, the EU also implemented the E-Privacy Directive ("EPD").[148] The EPD requires that companies based in Europe with web-based business and those with business directed at European Union citizens must request consent before they can install cookies.[149] This Directive, however, does not apply to cookies that are essential to basic functionality of the website, as use of the site in the first place implies consent.[150]

Since many other countries also have their own umbrella privacy laws, this results in increased compliance costs for corporations as they seek to conduct business internationally. Some countries have further developed laws to facilitate transfer of information with foreign countries. The cooperation of the United States Department of Commerce and the European Commission developed the "Safe Harbor" Framework to provide for an efficient manner for U.S. organizations to meet the Directive's "adequacy" requirement.[151] Safe Harbor "is a voluntary self-certification system for transmitting data from the EU to the United States" that essentially requires adoption of the Directive's "data quality principles" such that the personal data about European citizens transferred into the United States is treated as though it still remains in Europe.[152] The United

143. *Id.*

144. M LAW GRP., *supra* note 140.

145. Dixon, *supra* note 142.

146. *Id.*

147. M LAW GRP., *supra* note 140.

148. Bobbie Johnson, *What You Need to Know About EU Cookie Law*, GIGAOM (May 25, 2012), http://gigaom.com/2012/05/25/cookie-law-explainer/.

149. *Id.*

150. *Id.*

151. *U.S.-EU Safe Harbor Overview*, EXPORT.GOV, http://www.export.gov/safeharbor/eu/eg_main_018476.asp (last visited Apr. 1, 2015).

152. Wolf & Tobin, *supra* note 128, § III.I.

States Department of Commerce maintains a public list of all U.S. organizations that have self-certified to the Safe Harbor Framework, which they are required to do annually.[153] Further, an organization must state in its privacy policy statement that it complies with the Safe Harbor Privacy Principles.[154] The Asian-Pacific Economic Cooperation ("APEC") developed Cross Border Privacy Rules by 2011 and, thereafter, the United States and Mexico became the first countries to join this system.[155] The system utilizes third party "accountability agents" to ensure sufficiency of the organization's data privacy policies and practices.[156] Specifically, the United States has named TRUSTe as an "accountability agent" and empowered the FTC with enforcement authority.[157]

The FTC has acknowledged that the number of recent "incidents of unauthorized or improper use and sharing of personal information" indicate that companies mindful of consumer privacy lack sufficiently clear standards for guidance.[158] Further, companies that knowingly violate consumer privacy are not legally incentivized to prevent such actions.[159] The FTC has brought more than forty data security cases thus far on the basis of unfairness and deception.[160] On August 19, 2013, in the keynote prepared by the FTC for the Technology Policy Institute Aspen Forum, Chairwoman Edith Ramirez recognized the vast potential of Big Data and assured that the "FTC will remain vigilant to ensure that while innovation pushes forward, consumer privacy is not engulfed."[161] In doing so, she essentially suggested an expansion of the FTC's power to ensure that advancements in Big Data are "sufficiently rigorous privacy safeguards."[162]

153. EXPORT.GOV, *supra* note 150.

154. *Id.*

155. *The Cross Border Privacy Rules System: Promoting Consumer Privacy and Economic Growth Across the APEC Region,* APEC (Sept. 5, 2013), http://www.apec.org/Press/Features/2013/0903_cbpr.aspx.

156. *Id.*

157. *Id.*

158. FTC REPORT ON PROTECTING CONSUMER PRIVACY, *supra* note 95, at 12.

159. *Id.*

160. *Id.* at 2.

161. Ramirez, *supra* note 1, at 10.

162. *Id.* at 4.

III. Analysis

The United States lacks a comprehensive baseline federal standard of online privacy laws regulating collection, utilization, transfer, and deletion of consumer data, and providing consumer access to such data.[163] In its 2012 report, the FTC acknowledged what it described to be "ubiquitous data collection" and called on companies to limit such practices to data that is essential to perform the service or transaction for the consumer.[164] As discussed in Part II above, the vast majority of companies have been using collected information for purposes other than the specific purpose for which they were allowed to access the information. Since the FTC does not currently require companies to declare to customers precisely the manner in which their data is being utilized, even vigilant consumers are left vulnerable.[165] Even if consumers can learn that their information has been collected, bought, or sold without their permission, they have no statutory right to demand that such information be deleted.[166]

Further, the government has been struggling to keep up with the rapid evolution of modern technology.[167] The ability to efficiently mine through information has made the process of re-identification a simple process of running searches amongst two databases—one with de-identified personal information and one with identified information—until a commonality is found linking the de-identified information back to the individual.[168] Companies are consistently developing new ways to track consumers and collect data.[169] This practice is best exemplified by Acxiom's September 2013 announcement that its "Audience Operating System" would replace work done by third-party cookies as it would "combine data from multiple sources and enable digital marketers to segment and target audiences across channels and devices."[170]

163. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO 13-663, CONSUMER PRIVACY FRAMEWORK NEEDS TO REFLECT CHANGES IN TECHNOLOGY AND THE MARKETPLACE 7 (2013), *available at* http://www.gao.gov/assets/660/658151.pdf.

164. FTC REPORT ON PROTECTING CONSUMER PRIVACY, *supra* note 95, at 33.

165. *Testimony of Deirdre Mulligan before the Senate Committee on Commerce, Science and Transportation Subcommittee on Communications*, CTR. FOR DEMOCRACY AND TECH. (Sept. 23, 1998), https://www.cdt.org/issue/baseline-privacy-legislation.

166. *Id.*

167. *Id.*

168. ELEC. PRIVACY INFO. CTR., *Re-identification*, *supra* note 14.

169. *Id.*

170. U.S. SENATE, OFFICE OF OVERSIGHT AND INVESTIGATIONS MAJORITY STAFF, A REVIEW OF THE DATA BROKER INDUSTRY: COLLECTION, USE, AND SALE OF CONSUMER DATA FOR MARKETING PURPOSES 31 (2013), *available at* http://educationnewyork.com/files/rockefeller_databroker.pdf.

A. Ineffectiveness of Section 5 of the FTCA

The use of section 5 of the FTCA, coupled with an emphasis on self-regulation, to address online privacy issues is an ineffective enforcement mechanism because of the section's vague wording and the FTC's consistent struggle to establish its authority through precedent. Many companies have questioned the FTC's authority due to the ambiguity of section 5 of the FTCA.[171] Section 5 does not explicitly empower the FTC with jurisdiction over information security and informational privacy.[172] Most notably, the FTC acknowledges its lack of authority to mandate that firms adopt "information practice policies or to abide by the fair information practice principles on their Web sites, or portions of their Web sites, not directed at children."[173] Without such authority, no viable claim exists under the "deceptive" prong of the FTC's authority.[174] Further, the definition of "unfairness" does not provide companies guidance on what specifically constitutes acceptable practices with respect to consumer privacy.[175] As a result, companies are left with conjecture and speculation, as no law guides them on what practices are acceptable, and the only available references they have are "FTC recommendations, guides, reports, and policy statements . . . and consent orders from FTC settlements."[176]

Moreover, the FTCA deprives individuals of a private right of action against companies for misappropriating such information, and individuals cannot force the FTC to act on their behalf.[177] The FTC has even requested that Congress create civil penalties for companies that do not take reasonable measures to protect Big Data.[178]

Divergent views exist when addressing whether self-regulation is effective and whether more comprehensive legislation is required. Supporters of self-regulation have emphasized the voluntary industry measures that have taken place without further legislation, flexibility of the method that allows the industry to easily adapt to changes in technology, in comparison to lengthy process of enacting a law, and increased compliance

171. Jay Levine, *LabMD Joins Wyndham in Challenging FTC's Data Privacy Authority*, TECH. LAW SOURCE (Dec. 5, 2013), http://www.technologylawsource.com/2013/12/articles/hitech-act-compliance/labmd-joins-wyndham-in-challenging-ftcs-data-privacy-authority/.

172. *Id.*

173. FTC REPORT ON FAIR INFORMATION PRACTICES, *supra* note 82, at 34.

174. *Id.*

175. *See* FTC REPORT ON PROTECTING CONSUMER PRIVACY, *supra* note 95, at C-1 (Commissioner Rosch's dissent to the FTC's 2012 Privacy Report, noting that "unfairness is an elastic and elusive concept").

176. Friel, *supra* note 79.

177. *Overview of Statutory Authority to Remedy Privacy Infringements*, ELEC. PRIVACY INFO. CTR., http://epic.org//privacy/internet/ftc/Authority.html#fn1 (last visited Jan. 10, 2014).

178. Ramirez, *supra* note 1, at 6.

costs that it would potentially entail.[179] Additionally, self-regulation promotes innovation amongst the online-marketing industry.[180] On the other hand, critics of self-regulation have pointed to the process's failure in that privacy policies that entail data collection and use practices are usually lengthy and consumers often do not read them.[181] Further, a question exists as to whether an average individual reading a privacy policy would understand it sufficiently to make an informed choice.[182] Critics highlight that information resellers and other companies lack transparency, and they do not provide much information to consumers regarding their data practices.[183]

Advocates for baseline legislation argue that it would fill voids left by the current sectorial approach, provide for uniformity amongst the States, and benefit businesses by reducing costs of complying with the various laws.[184] Additionally, other countries would be more comfortable cooperating with the United States.[185] Critics of baseline legislation emphasize the inability of legislation to cater to the vast array of industry practices.[186] Although a detailed law would be difficult to apply across various industries and to adapt to evolving technologies, a law that is too vague could leave companies without proper guidance as to what practices would be acceptable.[187]

B. Recommendations

There are limitations on personal record-keeping practices to prevent federal agencies from intruding into personal privacy, but the lack of generally applicable data privacy rules to restrict the private sector appears to be an alarming inconsistency.[188] Although baseline legislation is preferred for purposes of clarity and uniformity, it may immediately hamper innovation and place significant burdens on businesses.[189] As existing privacy laws already provide effective tailored solutions to specific situations, adopting conflicting legislation would also be ineffective.[190]

179. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 163, at 28, 29, 43.

180. Thomas H. Davenport, *Should the U.S. Adopt European-Style Data Privacy Protections*, WALL ST. J., Mar. 10, 2013, *available at* http://www.wsj.com/articles/SB10001424127887324338604578328393797127094.

181. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 163, at 33.

182. *Id.*

183. *Id.*

184. *Id.*

185. *Id.* at 33.

186. *Id.* at 34.

187. *Id.* at 5.

188. DEP'T OF COMMERCE INTERNET POLICY TASK FORCE, *supra* note 17, at 11.

189. *Id.* at 4.

190. *Id.* at 58.

However, as many cases depict the failure of self-regulation and since the government has delayed in adopting baseline legislation, an effective approach would entail the adoption of preliminary legislation while Congress considers broader baseline legislation. These enactments would be incremental in comparison to broader baseline legislation but would better align the United States' privacy laws with that of other states, improve consumer confidence, and would be cost effective to broader legislation.

1. Heighten Transparency

The first step in enacting legislation geared towards online privacy should focus on transparency in data collection and use practies. Congress should enact a law similar to the California Right to Know Act, Assembly Bill 1291.[191] This bill provides that companies must reveal, upon request, all information they have collected about an individual and the manner in which they utilize such information.[192] The bill requires that companies provide accounting once every twelve months and incentivizes compliance via statutory penalties, providing that failure to comply "constitutes an injury to a customer."[193] In addition, mandating companies to undertake privacy impact assessments to "evaluate privacy risk arising from the use of personal information in new technologies or information practices" would create self-awareness for the companies and, if made public, would raise consumer awareness.[194] It is essential that companies inform consumers of the true costs for keeping many of their favorite sites free.

2. Incentivize Compliance

Instead of the current focus on disciplining companies when incidents occur, the government should incentivize companies to take measures to ensure that no such breaches occur in the first place. To incentivize companies to take preventative measures, Congress should implement a "token economy system," which is essentially the use of rewards to positively reinforce a desired behavior.[195] Congress could also establish a committee to conduct investigations of the data security measures taken by

191. A.B. 1291, 2013-2014 Reg. Sess., CAL. CIV. CODE § 1798.83 (Cal. 2013).

192. See Mauricio F. Paez, *Do You Know California's "Right to Know Act of 2013"?* JONES DAY (Apr. 2013), http://www.jonesday.com/do_you_know_california/, for more information on California's approach to protecting online privacy.

193. *Id.*

194. DEP'T OF COMMERCE INTERNET POLICY TASK FORCE, *supra* note 17, at 34.

195. TABER'S CYCLOPEDIC MEDICAL DICTIONARY 2330 (22d ed. 2013); ATTORNEYS' TEXTBOOK OF MEDICINE § 12-104, ch. 104.24(2).

various online companies, accordingly rate such companies, and make their conclusions available to the public.

3. Re-define the FTC's Enforcement Authority

It is vital that Congress re-define the FTC's enforcement authority role to explicitly encompass online privacy practices, self-regulatory efforts, and future legislation enacted in the realm of online privacy.[196] Congress should also require an auditing process to ensure that a company's privacy policies comply with fair information practices and that the company commits no misconduct.[197] Conducting audits randomly, rather than periodically, would support consistent compliance and minimize the costs as audits can be performed less frequently.

4. Limit the Amount of Information Collected

To better align with foreign nations, such as European countries and Canada, Congress should place some form of limitations on the amount of information collected. The FTC's refined "context of interaction" approach strikes a reasonable balance between innovation and privacy by taking an objective approach to determine whether a consumer should be provided choice in data collection. As the data collected via the "context of the interaction" approach is contextually focused on the purpose for which the data is collected, it would align well with Canada's PIPEDA and the EU's Directive as they are also purpose-oriented.[198]

5. Make Websites Post Data Collection Techniques and Types of Data Collected

An effective step towards limiting the ability of companies to circumvent a user's preference for online anonymity would require them to specify on their websites the technology they use to collect data and the type of data collected. To achieve uniformity and clarity amongst the online commercial entities that collect data, Congress should mandate standardized templates for online companies to draft their privacy policies much analogous to the manner in which the Insurance Service Office develops contracts for use by insurers.[199] Although this approach would not be as strict as the EPD's requirement that companies request permission before installing cookies, it will nonetheless create awareness. Further, it

196. DEP'T OF COMMERCE INTERNET POLICY TASK FORCE, *supra* note 17, at 62.

197. *Id.* at 61.

198. FTC REPORT ON PROTECTING CONSUMER PRIVACY, *supra* note 95, at 39.

199. *ISO Line-of-Insurance Programs*, VERISK ANALYTICS, http://www.verisk.com/products-and-services/product-category/policy-language-and-rules/iso-line-of-insurance-programs-loss-costs-rules-policy-forms.html (last visited Apr. 1, 2015).

would be a manner of holding companies accountable and encouraging them not to use malicious technology for fear of losing consumer trust.

6. Adopt the U.S. Commerce Department's Recommendation to Establish a Privacy Policy Office

Another effective step would be to fulfill the recommendation by the United States Department of Commerce that Congress should utilize existing resources to establish a Privacy Policy Office to focus solely on commercial data privacy.[200] The Privacy Policy Office would cooperate with the FTC and other existing agencies to organize various stakeholders for purposes of providing solutions to commercial data privacy issues and provide guidance to the industry as a whole.[201] Notably, establishing the Privacy Policy Office would be a flexible approach, as it would help develop voluntary and enforceable commercial data privacy codes pertaining to newly developed technologies.[202] Bringing stakeholders and this regulatory agency together is the best way to develop codes of conduct, as negotiation would likely strike an efficient balance between government involvement and self-regulation.

IV. Conclusion

Congress's sectorial approach to online privacy, along with an emphasis on self-regulation, has failed to provide consumers with adequate protection with respect to the collection, utilization, and transfer of personal data. Congress has failed to keep pace with the immense amount of personal data being generated from innovative technology that is geared towards delivering a personal experience to each customer. Additionally, enacting baseline legislation may take a while, as it would have immense effects on a broad array of stakeholders and would need to accurately draw a fine line between protection of privacy and encouraging innovation. Congress will further have to consider the many different state and international data privacy laws that currently exist. Compliance with these various laws is, however, currently burdensome to American businesses and is detrimental to the economy. Thus, Congress should take preliminary steps to better strike a balance between consumers' constitutional right to privacy and international economic growth by enacting legislation pursuant to key recommendations of the FTC and the United States Department of Commerce. Congress must act immediately to increase transparency to raise consumer awareness, incentivize companies to take preventative

200. DEP'T OF COMMERCE INTERNET POLICY TASK FORCE, *supra* note 17, at 46.
201. *Id.*
202. *Id.*

measures, implement an auditing process to ensure compliance, strengthen the FTC's enforcement role to hold companies liable for their actions, and establish a Privacy Policy Office to ensure privacy legislation keeps pace with the rapid evolution of technology.